HEALTH AFFAIRS

TRICARE
Management
Activity

MHS HIPAA Security: Incident Response Plan and Measuring Effectiveness

HIPAA Training: 2005 Summer Sessions

TMA Privacy Office

This document contains proprietary information and will be handled within Government regulations. It is intended solely for the use and information of the Military Health System.

Agenda

- Incident Response Plan
  - Background Information
  - Roles and Responsibilities
  - HIPAA Security Incident Response Procedures
  - HIPAA Security Incident Reporting

- Measuring Effectiveness
  - Background Information
  - HIPAA Security Reporting Elements
  - HIPAA Security Metrics
  - Measuring Ongoing Effectiveness

Training Objectives

- Upon completion of this course, you should be able to:
  - Identify the individuals and steps involved during a HIPAA security incident under the MHS HIPAA Security Incident Response Plan
  - Classify and report HIPAA security incidents as described in the MHS HIPAA Security Incident Response Plan
  - Measure and improve compliance with and management of HIPAA security

Incident Response Plan (IRP)

Incident Response Plan

Objectives

- Upon completion of this lesson, you should be able to:
  - Identify some of the key responsibilities and duties of the organizational staff that may be involved in managing and reporting HIPAA security incidents
  - Identify the types of security incidents that qualify as reportable incidents and, based upon the severity of the event, require notification of officials within TMA/MHS
  - Outline the structure and process for reporting HIPAA security incidents

Background Information

Requirement

- An administrative safeguard specified in the HIPAA Security Rule requires the development and implementation of policies, procedures, and processes for managing, responding to, and reporting security incidents

Background Information

Why Does DoD Need an IRP?

- DoD policies and procedures provide guidance pertaining to the security and handling of sensitive information within DoD organizations

- These documents do not specifically address the reporting process or procedures that are unique to a HIPAA security incident

Background Information

Purpose

- This Incident Response Plan:
  - Addresses the reporting process and procedures that are unique to a HIPAA security incident
  - Serves as a supplement to existing organizational information management and information security regulations, policies, and procedures

Roles and Responsibilities

Roles and Responsibilities

Objectives

- Upon completion of this module you should be able to:
  - Identify some of the key responsibilities and duties of the organizational staff that may be involved in managing and reporting HIPAA security incidents

Roles and Responsibilities

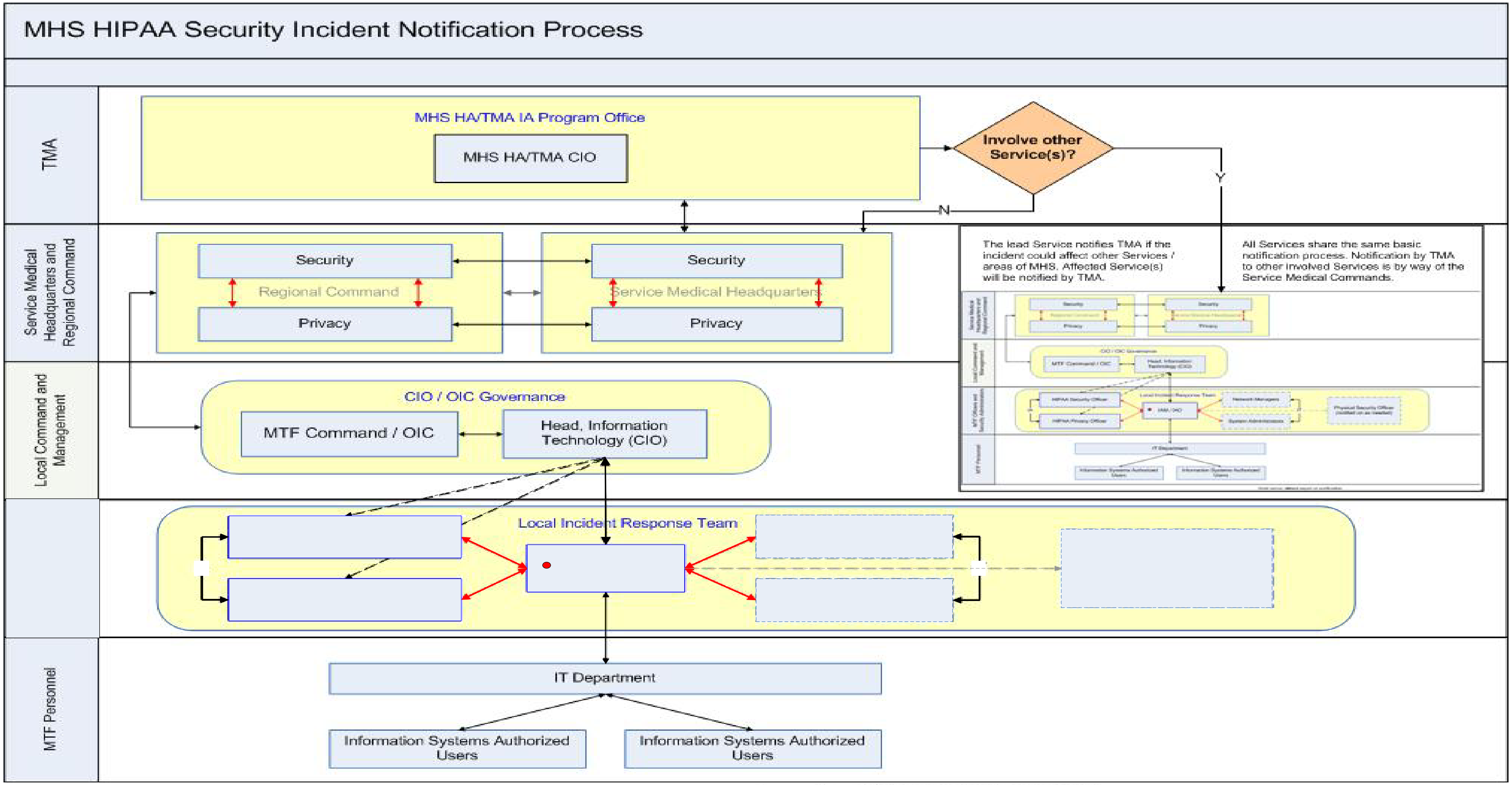
Severity Levels

- Severity levels 1 through 5 are used to classify HIPAA security incidents
  - Level 1 is the most severe
  - Level 5 is the least severe
- Severity level 3, 4 and 5 must be reported on a quarterly basis
- Severity level 2 must be reported to the Service Medical Headquarters on a monthly basis
- Severity level 1 must be reported to TMA within 24 hours of a HIPAA security incident

1
2
3
4
5

Roles and Responsibilities

Local Security Incident Response Team (SIRT) (1 of 3)



MHS HIPAA Security Incident Notification Process

TMA

MHS HA/TMA IA Program Office

MHS HA/TMA CIO

Involve other Service(s)?

Y

N

Service Medical Headquarters and Regional Command

Security

Regional Command

Privacy

Security

Service Medical Headquarters

Privacy

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

Local Command and Management

CIO / OIC Governance

MTF Command / OIC

Head, Information Technology (CIO)

Local Incident Response Team

MTF Personnel

IT Department

Information Systems Authorized Users

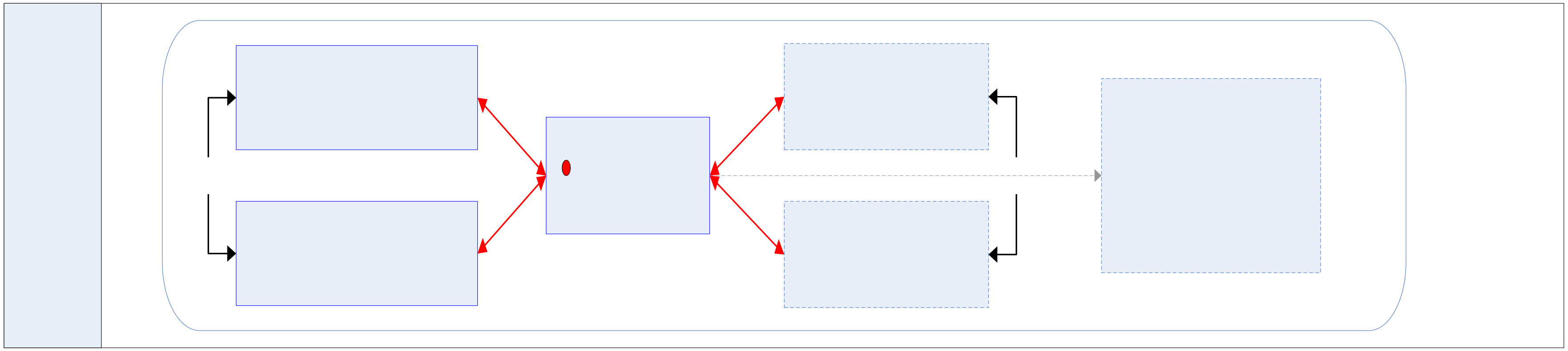
Information Systems Authorized Users

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

⟶	Solid arrow: **direct** report or notification
- - →	Dashed arrow: indicates **possible** notification, based on analysis of incident.
🟥⟶	Red arrow: indicates critical notification based on analysis of impact and severity
🟨	Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

Local Security Incident Response Team (SIRT) (2 of 3)



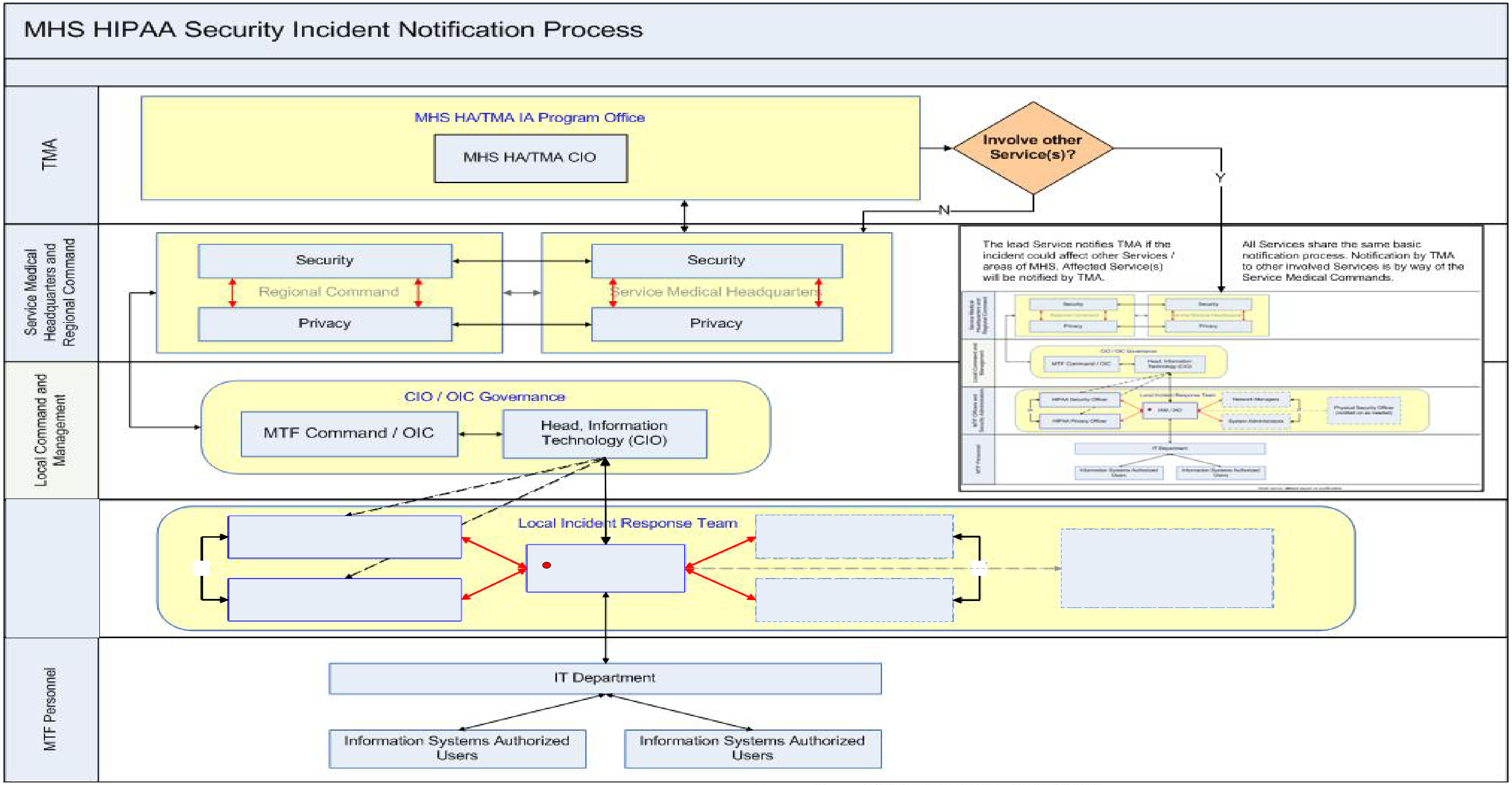
Roles and Responsibilities

Local Security Incident Response Team (SIRT) (3 of 3)

- The local SIRT is an extension of the local Computer Incident Response Team (CIRT) that includes:
  - Local HIPAA Security Officer
  - Local HIPAA Privacy Officer
  - Local Physical Security Officer
- Investigates security incidents at the direction of the Information Assurance Manager (IAM)/Information Assurance Officer (IAO)
- Provides recommendation on the severity level of an incident to the IAM/IAO

Roles and Responsibilities

Local HIPAA Security Officer (1 of 3)



MHS HIPAA Security Incident Notification Process

TMA
MHS HA/TMA IA Program Office
MHS HA/TMA CIO
Involve other Service(s)?
Y
N
Service Medical Headquarters and Regional Command
Security
Regional Command
Privacy
Security
Service Medical Headquarters
Privacy
Local Command and Management
CIO / OIC Governance
MTF Command / OIC
Head, Information Technology (CIO)
Local Incident Response Team
MTF Personnel
IT Department
Information Systems Authorized Users
Information Systems Authorized Users

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

→ Solid arrow: **direct** report or notification

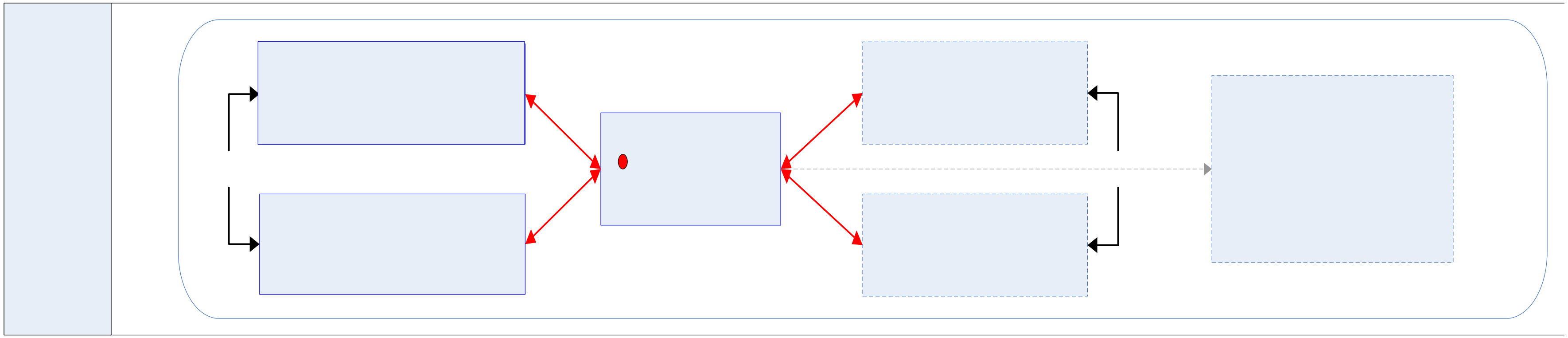
⇢ Dashed arrow: indicates **possible** notification, based on analysis of incident.

→ Red arrow: indicates critical notification based on analysis of impact and severity

▭ Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

Local HIPAA Security Officer (2 of 3)



Roles and Responsibilities

Local HIPAA Security Officer (3 of 3)

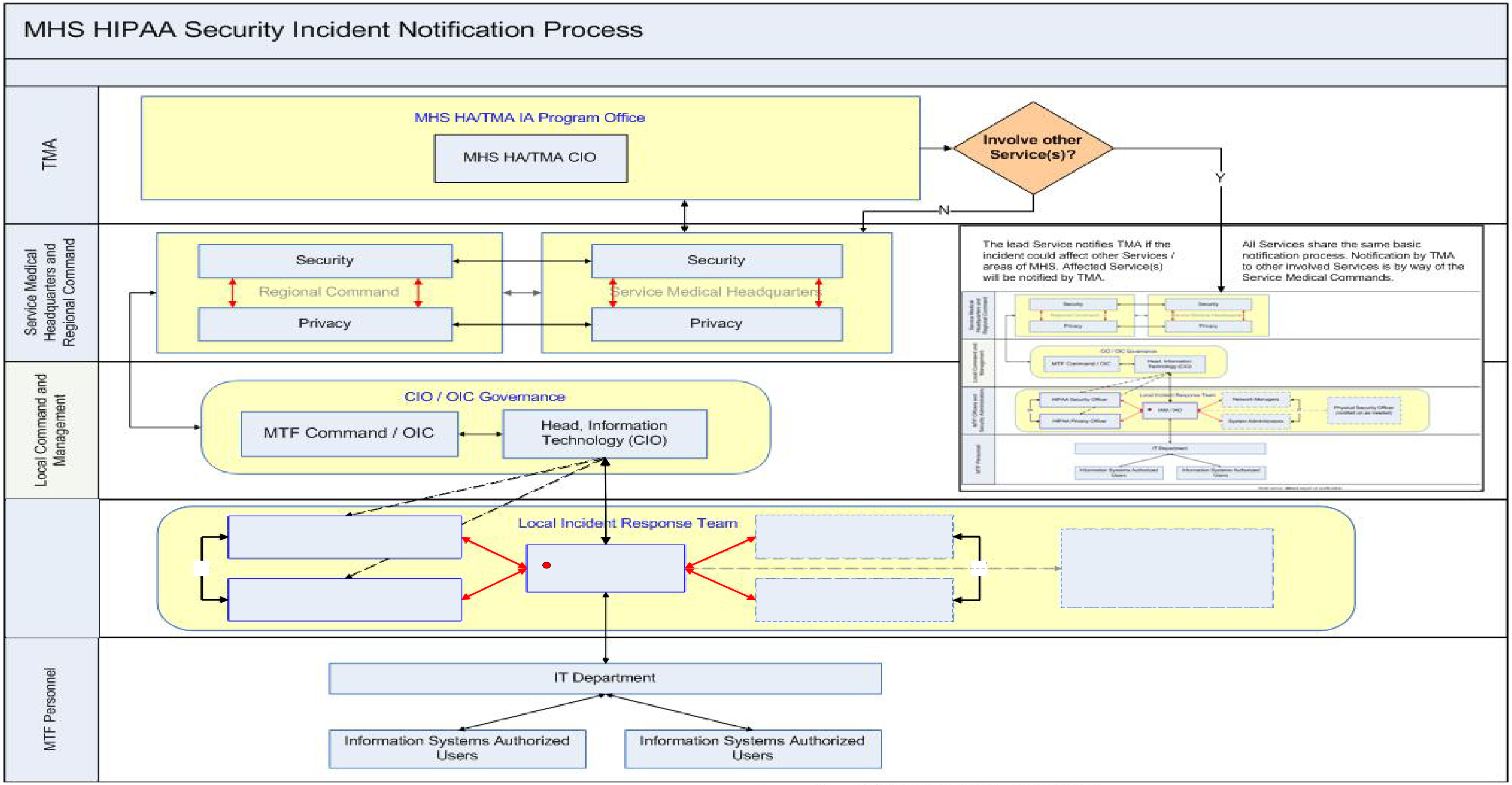
- Receives reports of security breaches, coordinates with other organizational staff to take appropriate action to minimize harm, investigates breaches and make recommendations to management for corrective action

- Participates on the local SIRT or other organizational teams, as necessary, to address HIPAA security incidents

- Works in conjunction with the local HIPAA Privacy Officer and Public Affairs Office (PAO)

Roles and Responsibilities

Information Assurance Officer (IAO)
Information Assurance Manager (IAM) (1 of 4)



MHS HIPAA Security Incident Notification Process

TMA

MHS HA/TMA IA Program Office

MHS HA/TMA CIO

Involve other Service(s)?

Y

N

Service Medical Headquarters and Regional Command

Security

Regional Command

Privacy

Security

Service Medical Headquarters

Privacy

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

Local Command and Management

CIO / OIC Governance

MTF Command / OIC

Head, Information Technology (CIO)

Local Incident Response Team

MTF Personnel

IT Department

Information Systems Authorized Users

Information Systems Authorized Users

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

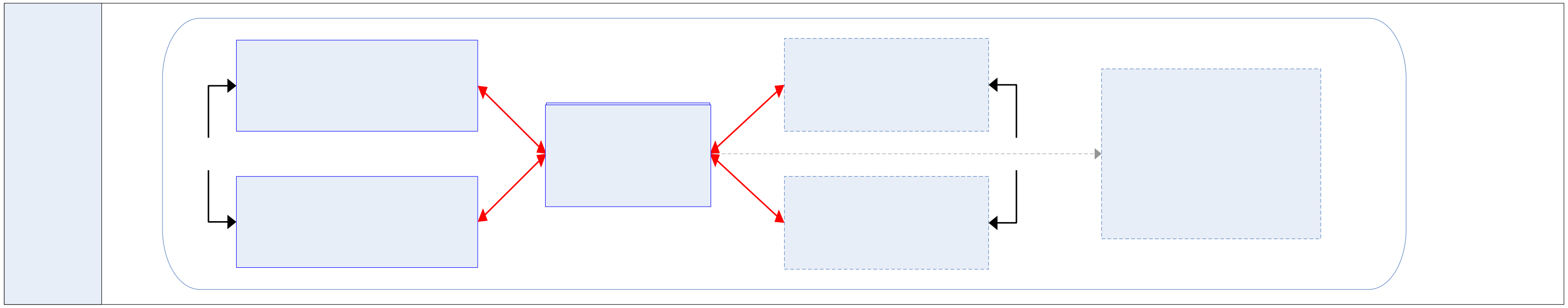
→ Solid arrow: **direct** report or notification

- - → Dashed arrow: indicates **possible** notification, based on analysis of incident.

→ Red arrow: indicates critical notification based on analysis of impact and severity

🟨 Grouping: presumes local procedures for maintaining communication and awareness

Information Assurance Officer (IAO) Information Assurance Manager (IAM) (2 of 4)



Roles and Responsibilities

Information Assurance Officer (IAO) Information Assurance Manager (IAM) (3 of 4)

- Creates the organizational incident response plan that addresses procedures and process to be followed to address HIPAA security incidents
- Identifies personnel to serve on the local SIRT
- Ensures local staff receives training on how to report and respond to a HIPAA security incident
- Receives notification of all HIPAA incidents as the central point of contact

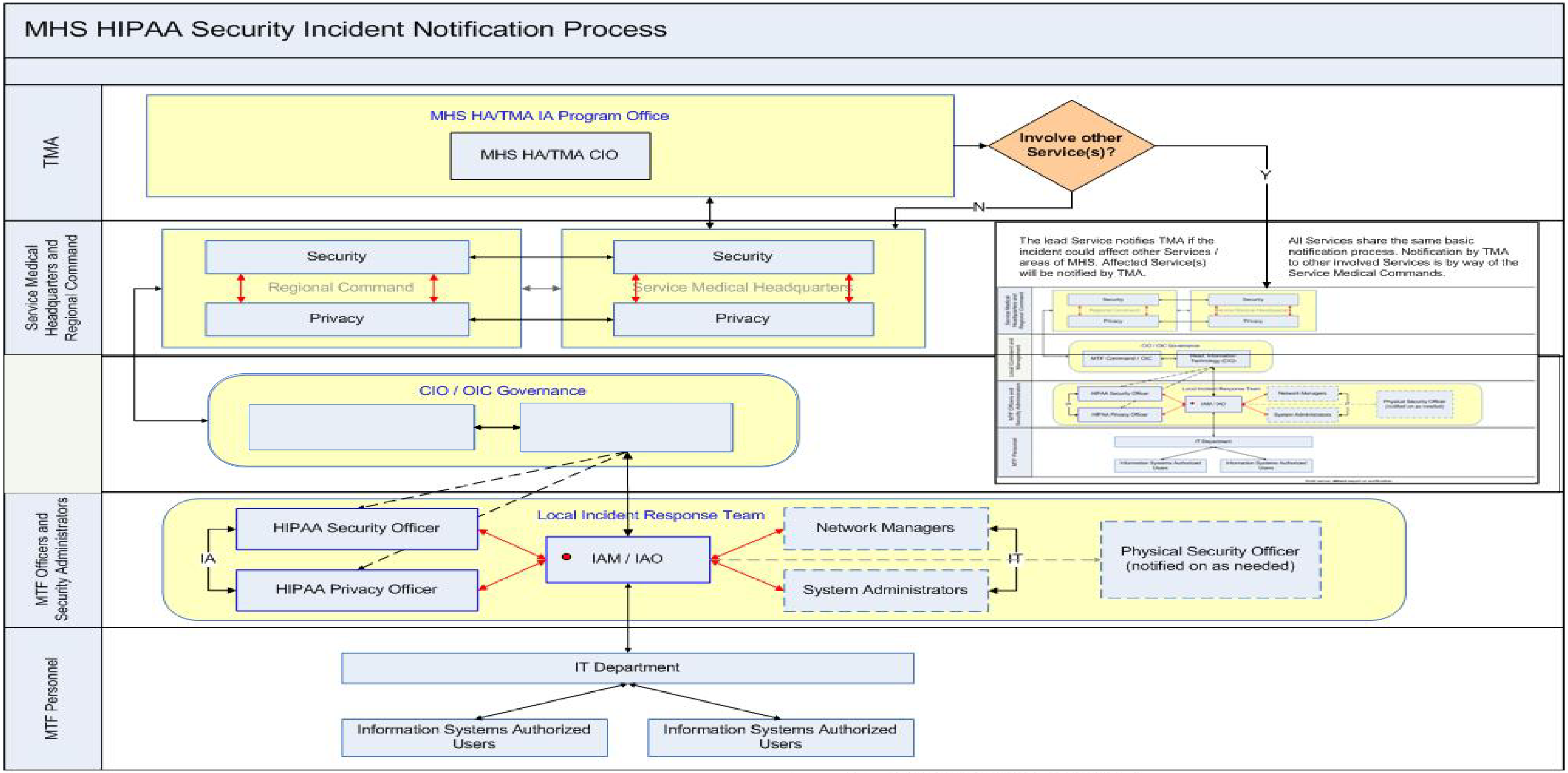
Roles and Responsibilities

Information Assurance Officer (IAO) Information Assurance Manager (IAM) (4 of 4)

- Coordinates the SIRT to investigate all HIPAA incidents
- Consults the local HIPAA Security and Privacy Officers to determine the nature and type of incident
- Determines the severity level based on analysis and recommendations of the SIRT
- Notifies and reports investigation findings to the Head of Information Technology (CIO)

Roles and Responsibilities

Head of Information Technology (CIO) (1 of 4)


MHS HIPAA Security Incident Notification Process
TMA
MHS HA/TMA IA Program Office
MHS HA/TMA CIO
Involve other Service(s)?
Y
N
Service Medical Headquarters and Regional Command
Security
Regional Command
Privacy
Security
Service Medical Headquarters
Privacy
CIO / OIC Governance
MTF Officers and Security Administrators
Local Incident Response Team
HIPAA Security Officer
IA
HIPAA Privacy Officer
IAM / IAO
Network Managers
IT
System Administrators
Physical Security Officer (notified on as needed)
MTF Personnel
IT Department
Information Systems Authorized Users
Information Systems Authorized Users

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

Solid arrow: **direct** report or notification

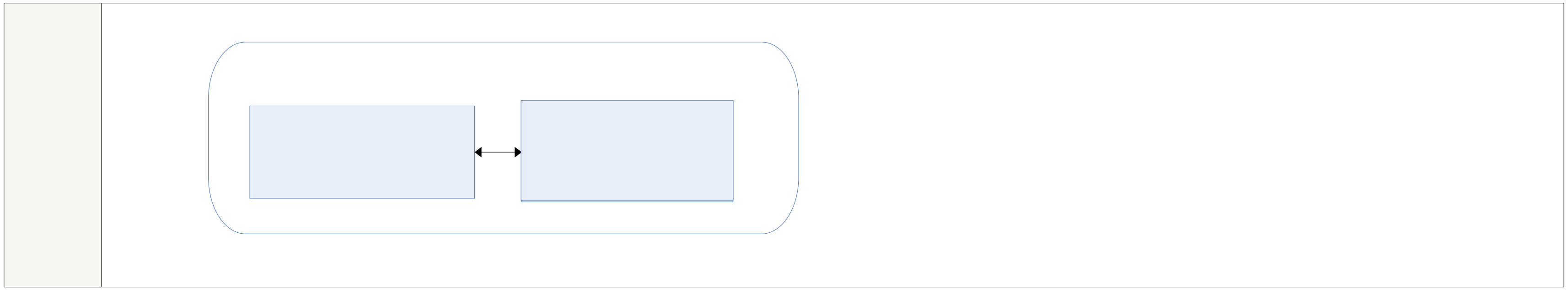
Dashed arrow: indicates **possible** notification, based on analysis of incident.

Red arrow: indicates critical notification based on analysis of impact and severity

Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

Head of Information Technology (CIO) (2 of 4)



Roles and Responsibilities

Head of Information Technology (CIO) (3 of 4)

- Ensures that identified HIPAA security incidents are properly documented and investigated

- Reports security incidents to regional and Service Medical Headquarters officials in conjunction with Military Treatment Facility (MTF) Commanders/Officers In Charge (OICs)

- Ensures that plans, processes, and procedures are in place for monitoring automated information systems and networks for attempts to subvert security controls

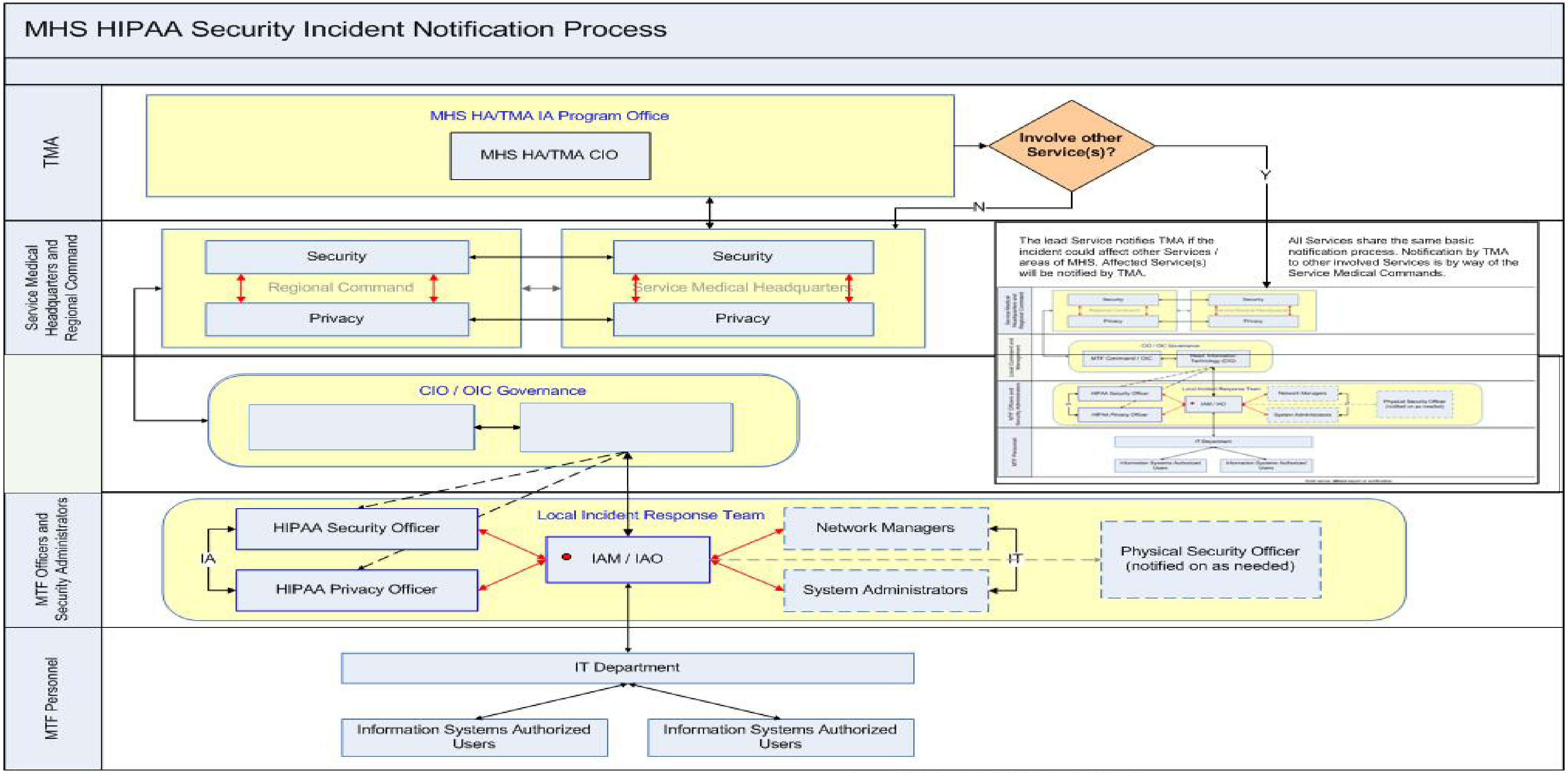
Roles and Responsibilities

Head of Information Technology (CIO) (4 of 4)

- In coordination with the IAM:
  - Advises the local HIPAA Security Officer of security anomalies or integrity deficiencies that may compromise the confidentiality, integrity, and availability of ePHI
  - Advises the local HIPAA Privacy Officer of any issues or security incidents that may result in an unauthorized use or disclosure of Protected Health Information (PHI)

Roles and Responsibilities

MTF Commanders/OICs (1 of 3)



MHS HIPAA Security Incident Notification Process

TMA

Service Medical Headquarters and Regional Command

MTF Officers and Security Administrators

MTF Personnel

MHS HA/TMA IA Program Office

MHS HA/TMA CIO

Involve other Service(s)?

Y

N

Security

Regional Command

Privacy

Security

Service Medical Headquarters

Privacy

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

CIO / OIC Governance

Local Incident Response Team

HIPAA Security Officer

IA

HIPAA Privacy Officer

● IAM / IAO

Network Managers

IT

System Administrators

Physical Security Officer (notified on as needed)

IT Department

Information Systems Authorized Users

Information Systems Authorized Users

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

→ Solid arrow: **direct** report or notification

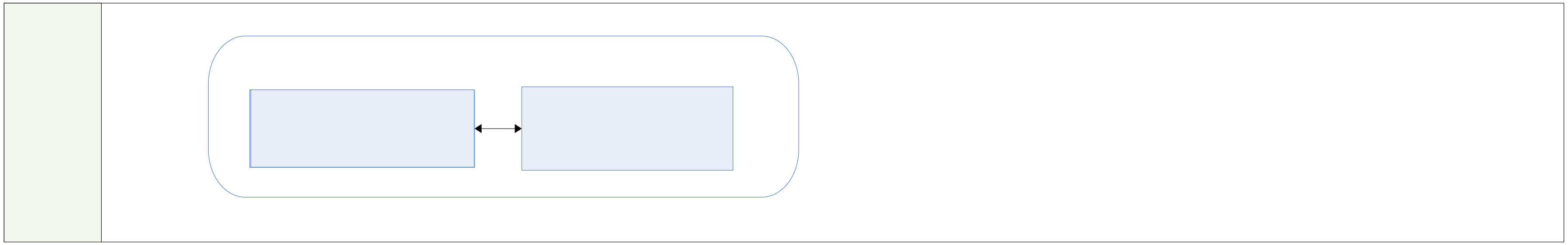
- - → Dashed arrow: indicates **possible** notification, based on analysis of incident.

→ Red arrow: indicates critical notification based on analysis of impact and severity

🟨 Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

MTF Commanders/OICs (2 of 3)



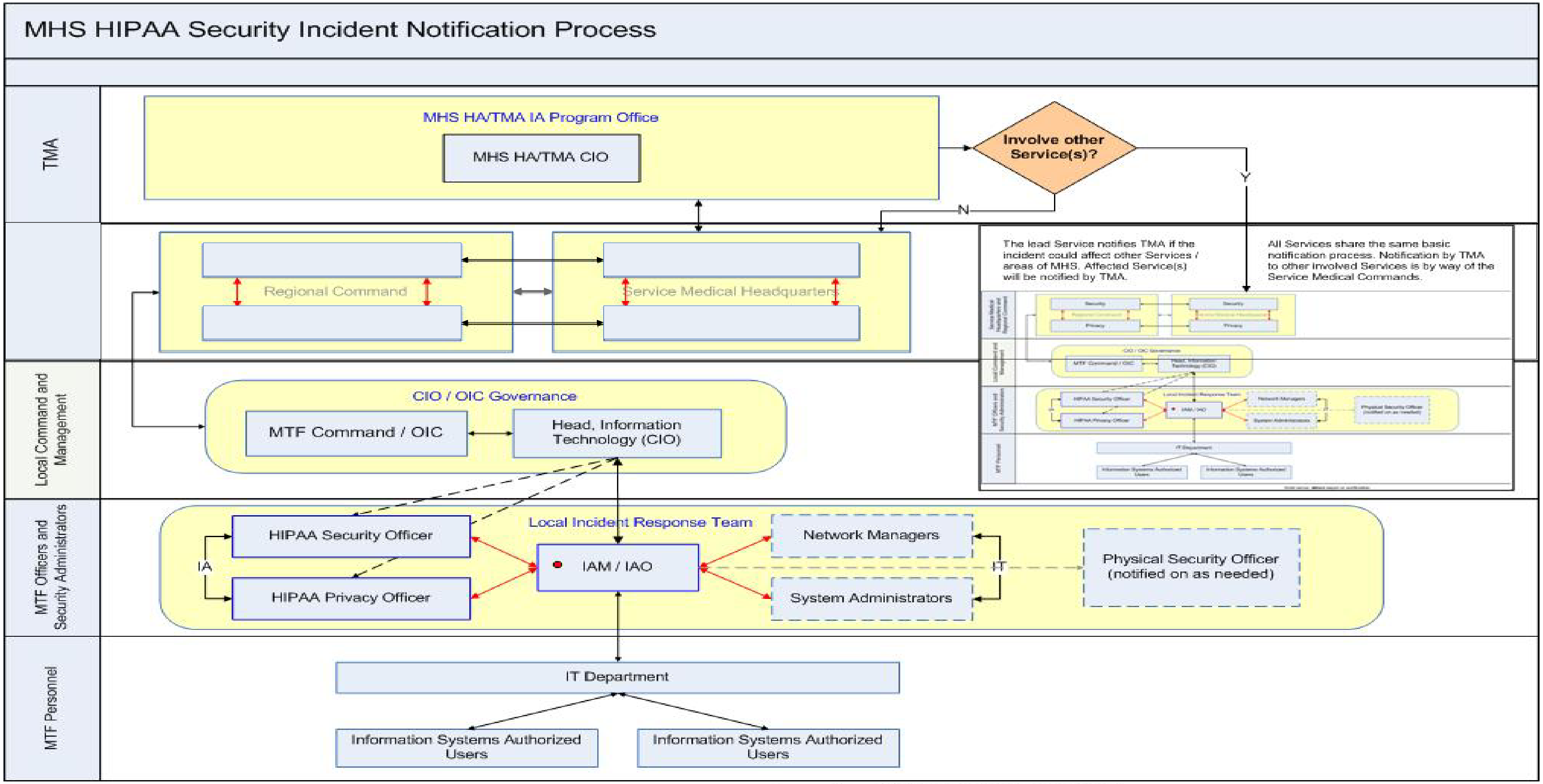
Roles and Responsibilities

MTF Commanders/OICs (3 of 3)

- Appoint appropriate personnel in writing to manage the HIPAA security requirements
- Responsible for the overall oversight, response, and reporting of HIPAA security incidents
- Ensure that the Command establishes a security incident response plan that includes information pertaining to management of HIPAA security incidents
- Ensure level 1 and 2 HIPAA security incidents are reported to regional and/or Service Medical Headquarters

Roles and Responsibilities

Regional Commands (1 of 4)



MHS HIPAA Security Incident Notification Process

TMA
Local Command and Management
MTF Officers and Security Administrators
MTF Personnel
MHS HA/TMA IA Program Office
MHS HA/TMA CIO
Involve other Service(s)?
Y
N
Regional Command
Service Medical Headquarters
CIO / OIC Governance
MTF Command / OIC
Head, Information Technology (CIO)
Local Incident Response Team
HIPAA Security Officer
HIPAA Privacy Officer
IA
IAM / IAO
Network Managers
System Administrators
IT
Physical Security Officer (notified on as needed)
IT Department
Information Systems Authorized Users
Information Systems Authorized Users

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

→ Solid arrow: **direct** report or notification

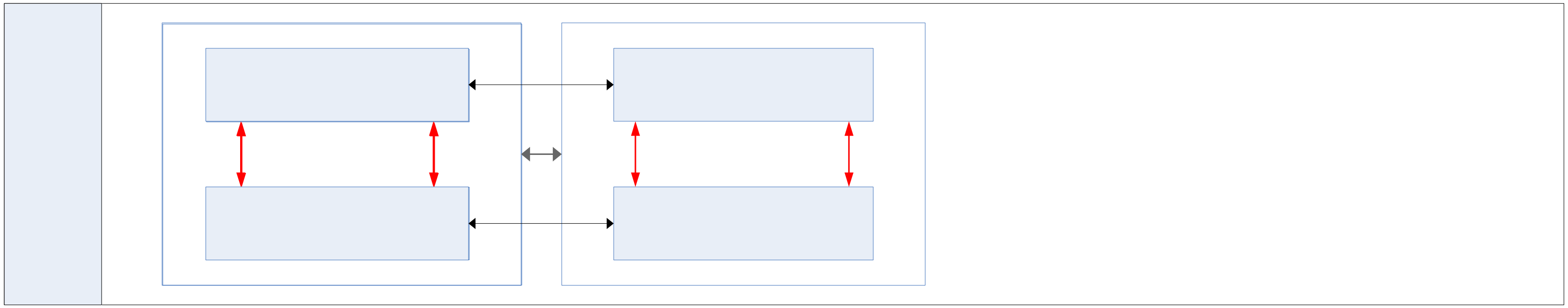
- - → Dashed arrow: indicates **possible** notification, based on analysis of incident.

→ Red arrow: indicates critical notification based on analysis of impact and severity

▭ Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

Regional Commands (2 of 4)



Roles and Responsibilities

Regional Commands (3 of 4)

- Receive reports of level 1 and 2 HIPAA security incidents from local commands and report this information to the Service Medical Headquarters

- Ensure Security and Privacy Officers within regional commands collaborate on the analysis and notification of security incidents

- Ensure identified HIPAA security incidents within regional commands are properly documented and investigated

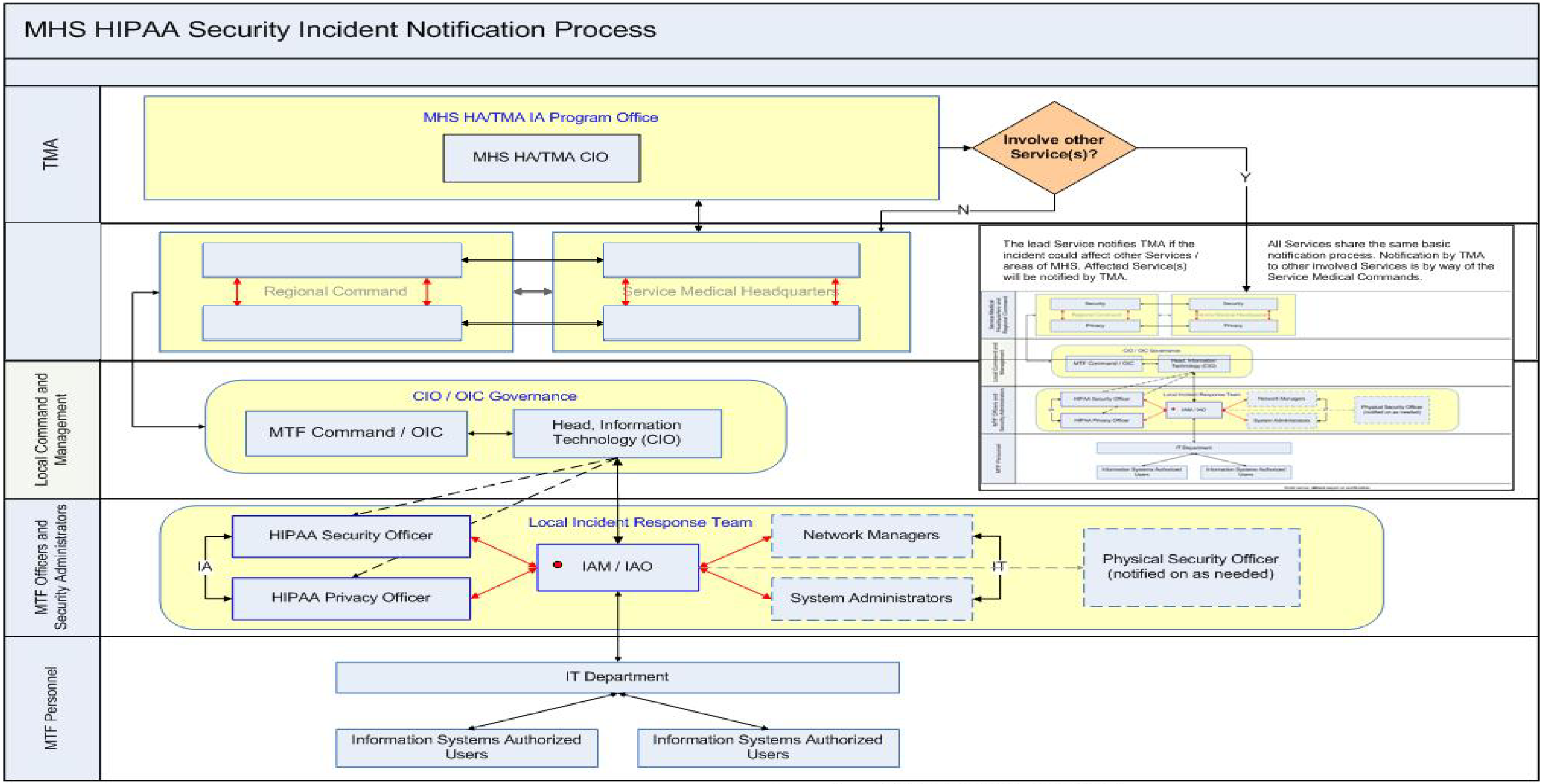
Roles and Responsibilities

Regional Commands (4 of 4)

- Ensure level 1 and 2 HIPAA security incidents within regional commands are reported to the Service Medical Headquarters

Roles and Responsibilities

Service Medical Headquarters (1 of 5)


MHS HIPAA Security Incident Notification Process
TMA
MHS HA/TMA IA Program Office
MHS HA/TMA CIO
Involve other Service(s)?
Y
N
Regional Command
Service Medical Headquarters
Local Command and Management
CIO / OIC Governance
MTF Command / OIC
Head, Information Technology (CIO)
MTF Officers and Security Administrators
Local Incident Response Team
HIPAA Security Officer
HIPAA Privacy Officer
IA
IAM / IAO
Network Managers
System Administrators
IT
Physical Security Officer (notified on as needed)
MTF Personnel
IT Department
Information Systems Authorized Users
Information Systems Authorized Users

The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.

All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

Solid arrow: **direct** report or notification

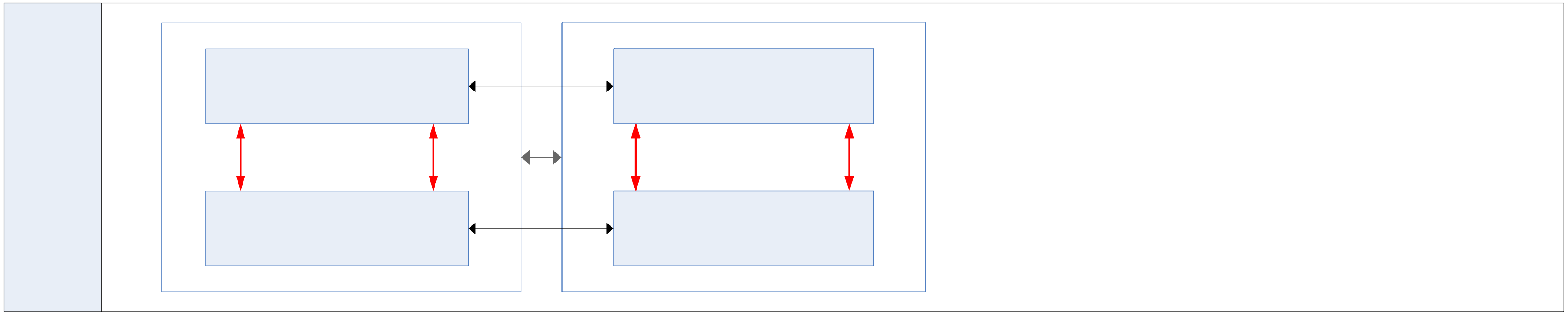
Dashed arrow: indicates **possible** notification, based on analysis of incident.

Red arrow: indicates critical notification based on analysis of impact and severity

🟨 Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

Service Medical Headquarters (2 of 5)



Roles and Responsibilities

Service Medical Headquarters (3 of 5)

- Receive reports of level 1 and 2 HIPAA security incidents from regional and/or local commands and report this information to the MHS HA/TMA IA Program Office in a manner consistent with the severity level

- Ensure that local commands establish a security incident response plan that includes guidance for reporting, responding to, and managing HIPAA security incidents

Roles and Responsibilities

Service Medical Headquarters (4 of 5)

- Ensure that other officials (internal and external to the organization) are notified of the incident
  - Public Affairs Office (PAO)
  - Legal Affairs Office
  - DoD Computer Emergency Response Team (CERT)

- Ensure both the Security and Privacy Officers in regional commands are notified commensurate with the severity level

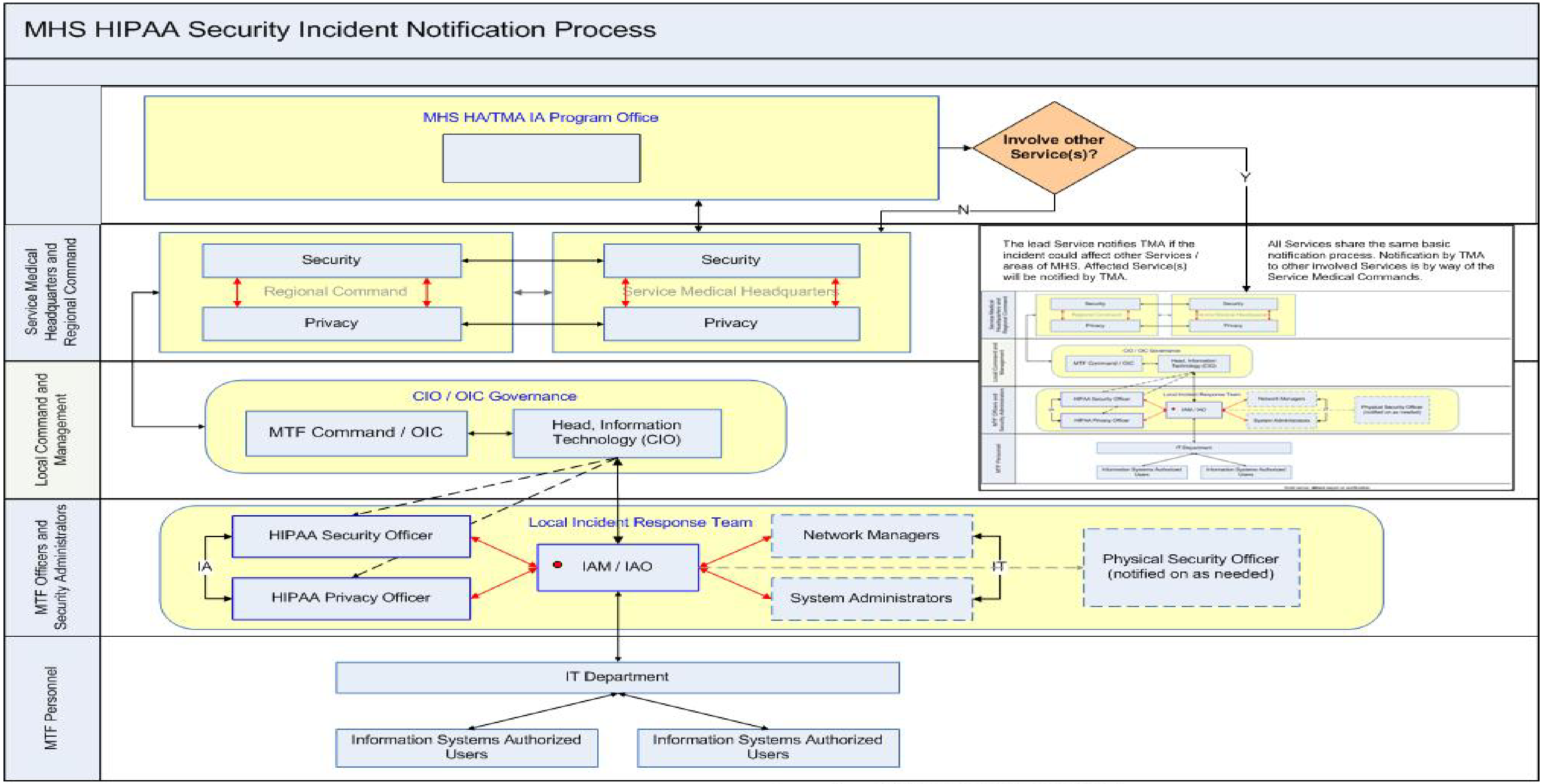
Roles and Responsibilities

Service Medical Headquarters (5 of 5)

- Ensure Security and Privacy Officers within the Service Medical Headquarters collaborate on the response, reporting, management analysis, and notification of incidents that occur at the local, regional, and/or Service Medical Headquarters level
- Ensure identified HIPAA security incidents within Service Medical Headquarters are properly documented and investigated
- Ensure level 1 and 2 HIPAA security incidents within the Service Medical Headquarters are reported to the MHS HA/TMA IA Program Office

Roles and Responsibilities

MHS HA/TMA IA Program Office (1 of 5)


MHS HIPAA Security Incident Notification Process
MHS HA/TMA IA Program Office
Involve other Service(s)?
Y
N
Service Medical Headquarters and Regional Command
Security
Regional Command
Privacy
Security
Service Medical Headquarters
Privacy
The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.
All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.
Local Command and Management
CIO / OIC Governance
MTF Command / OIC
Head, Information Technology (CIO)
MTF Officers and Security Administrators
Local Incident Response Team
HIPAA Security Officer
HIPAA Privacy Officer
IA
IAM / IAO
Network Managers
System Administrators
IT
Physical Security Officer (notified on as needed)
MTF Personnel
IT Department
Information Systems Authorized Users
Information Systems Authorized Users

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

→ Solid arrow: **direct** report or notification

- - → Dashed arrow: indicates **possible** notification, based on analysis of incident.

→ Red arrow: indicates critical notification based on analysis of impact and severity

▨ Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

MHS HA/TMA IA Program Office (2 of 5)

Roles and Responsibilities

MHS HA/TMA IA Program Office (3 of 5)

- Receives reports of level 1 and 2 HIPAA security incidents and take necessary action to ensure that all appropriate officials within TMA and civilian authorities are notified of the incident

Roles and Responsibilities

MHS HA/TMA IA Program Office (4 of 5)

- Provides assistance to the Service Medical Headquarters to assist in the management and response to HIPAA security incidents
  - Assists in determining the Services affected by the incident
  - Ensures security incidents are resolved
  - Ensures lessons learned are disseminated to all Services
  - Obtains a status of the level of media involvement and impact to affected information systems for all security incidents elevated to its office
  - Obtains an estimated cost associated with damage and risk mitigation for all level 5 security incidents

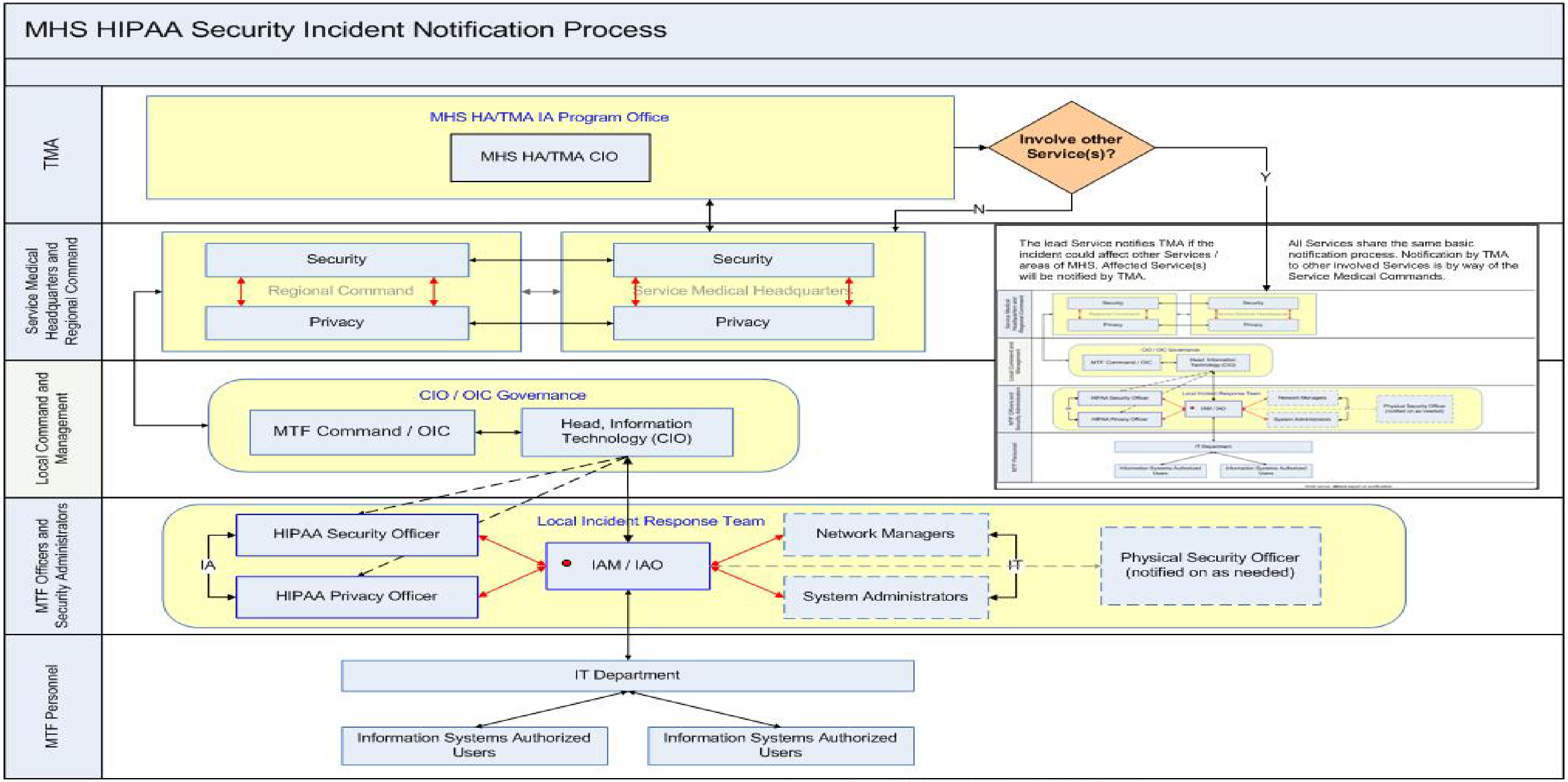
Roles and Responsibilities

MHS HA/TMA IA Program Office (5 of 5)

- Ensures the TMA Privacy Office is advised of:
  - All level 1 and 2 HIPAA security incidents
  - HIPAA security incidents that have privacy implications and/or involve an unauthorized or potential unauthorized disclosure of PHI
- Ensures coordination for resolution of incidents with the TMA Privacy Office
- Informs appropriate offices within TMA if patterns have been detected in quarterly reports that indicate vulnerabilities in centrally managed systems

Roles and Responsibilities

MHS HIPAA Security Incident Notification Process


MHS HIPAA Security Incident Notification Process
TMA
Service Medical Headquarters and Regional Command
Local Command and Management
MTF Officers and Security Administrators
MTF Personnel
MHS HA/TMA IA Program Office
MHS HA/TMA CIO
Involve other Service(s)?
Y
N
Security
Regional Command
Privacy
Security
Service Medical Headquarters
Privacy
The lead Service notifies TMA if the incident could affect other Services / areas of MHS. Affected Service(s) will be notified by TMA.
All Services share the same basic notification process. Notification by TMA to other involved Services is by way of the Service Medical Commands.
CIO / OIC Governance
MTF Command / OIC
Head, Information Technology (CIO)
Local Incident Response Team
HIPAA Security Officer
HIPAA Privacy Officer
IA
IAM / IAO
Network Managers
System Administrators
IT
Physical Security Officer (notified on as needed)
IT Department
Information Systems Authorized Users
Information Systems Authorized Users

● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

→ Solid arrow: **direct** report or notification

⇢ Dashed arrow: indicates **possible** notification, based on analysis of incident.

→ Red arrow: indicates critical notification based on analysis of impact and severity

🟨 Grouping: presumes local procedures for maintaining communication and awareness

Roles and Responsibilities

Summary

- You should now be able to:
  - Identify some of the key responsibilities and duties of the organizational staff that may be involved in managing and reporting HIPAA security incidents

HIPAA Security Incident Response Procedures

HIPAA Security Incident Response Procedures

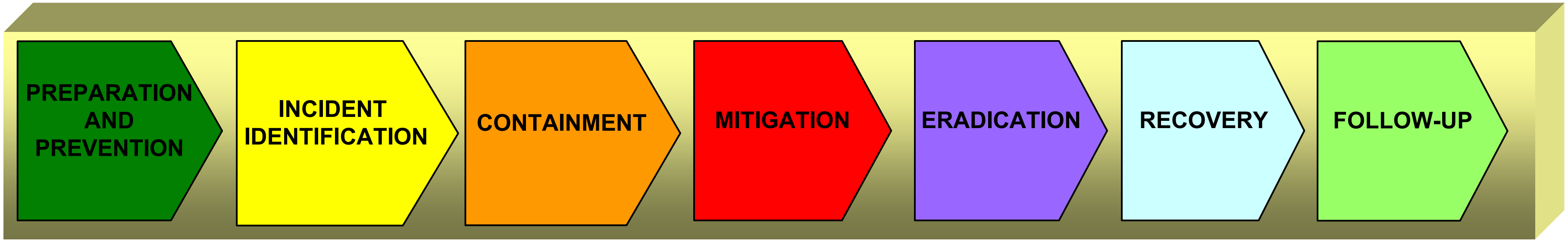
Objectives

- Upon completion of this module you should be able to:
  - Identify the types of security incidents that qualify as reportable incidents and, based upon the severity of the event, require notification of officials within TMA/MHS

HIPAA Security Incident Response Procedures

Procedures

- Local incident response plans should include, at a minimum:
  - Preparation and Prevention
  - Incident Identification
  - Containment
  - Mitigation
  - Eradication
  - Recovery
  - Follow-up

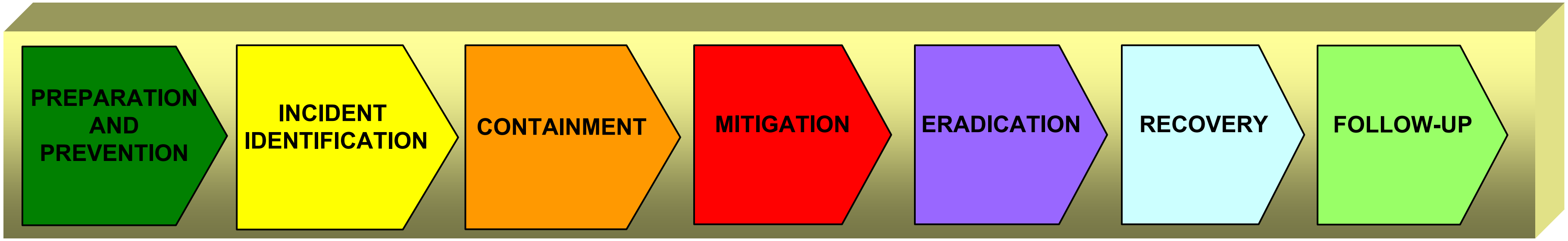


PREPARATION AND PREVENTION

HIPAA Security Incident Response Procedures

Preparation and Prevention

- Proper preparation will help organizations:
  - Respond to HIPAA security incidents
  - Prevent future incidents through the actions that are taken to secure ePHI


PREPARATION AND PREVENTION

INCIDENT IDENTIFICATION

CONTAINMENT

MITIGATION

ERADICATION

RECOVERY

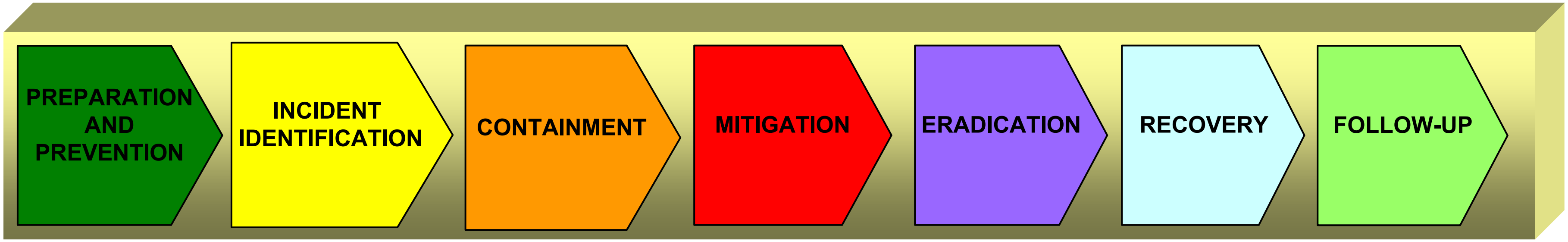
FOLLOW-UP

INCIDENT IDENTIFICATION

HIPAA Security Incident Response Procedures

Incident Identification (1 of 6)

- Incident identification involves the analysis of all available information in order to determine if a HIPAA security incident has occurred



HIPAA Security Incident Response Procedures

Incident Identification (2 of 6)

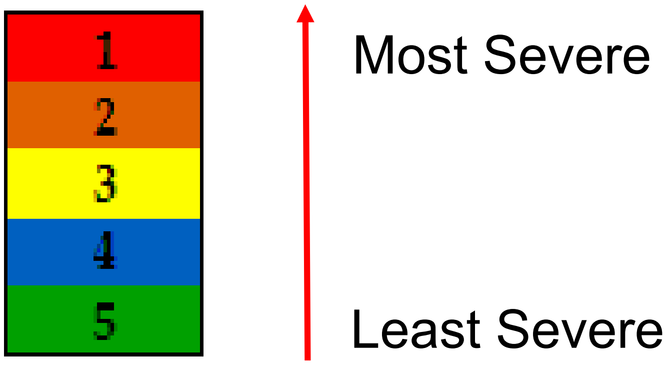
- Some situations that may indicate that a HIPAA security incident has occurred include:
  - – Unsuccessful login attempts
  - – An indicated last time of usage of a user account that does not correspond to the actual time of usage for the end user
  - – A privacy complaint that implicates an information system or network as the source of an unauthorized disclosure
  - – Sudden increase in unsolicited e-mail

HIPAA Security Incident Response Procedures

Incident Identification (3 of 6)

INCIDENT IDENTIFICATION

- Incident identification activities include, at a minimum, the following:
  - Classify the severity of the HIPAA security incident using the classification table provided in the Incident Response Plan
    - HIPAA security incident severity levels are classified on a scale of 1 through 5



INCIDENT IDENTIFICATION

HIPAA Security Incident Response Procedures

Incident Identification (4 of 6)

- ePHI Security Incident Severity Classification Table

SEVERITY LEVEL	DESCRIPTION	EXAMPLE
5	Small number of system probes or scans detected on external systems	The network administrator detects intermittent pinging activity to a router from an unknown source
	Isolated instances of known computer viruses easily handled by anti-virus software	Small number of trouble calls to the help desk reporting the detection of a common Microsoft Word macro virus by the anti-virus software
4	Small numbers of systems probes or scans detected on internal systems	The network administrator detects intermittent pinging activity to CHCS from an internal workstation
	Alerts received concerning threats to which systems may be vulnerable	Cyber security bulletins received from the US-CERT concerning the threat of a virus to which Microsoft Outlook may be vulnerable

HIPAA Security Incident Response Procedures

Incident Identification (5 of 6)

- ePHI Security Incident Severity Classification Table (Cont.)

SEVERITY LEVEL	DESCRIPTION	EXAMPLE
3	**Significant numbers of system probes or scans detected from internal or external sources**	**Regular pinging detected to CHCS for a sustained period of time**
	Penetration or denial of service attacks attempted with no impact on operations	**Unsuccessful login attempts to a router**
	Widespread instances of known computer viruses transmitted internally by users via e-mail easily handled by anti-virus software	**Users transmitting e-mails through Microsoft Outlook with attachments containing a virus previously reported**
	Isolated instances of a new computer virus not handled by anti-virus software detected only at one MTF	**Isolated trouble calls to the help desk reporting problems with Microsoft Outlook eventually found to be caused by the ILOVEYOU virus during its initial hours**

HIPAA Security Incident Response Procedures

Incident Identification (6 of 6)

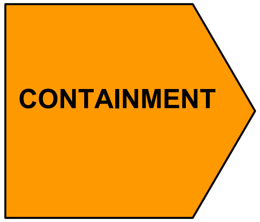
INCIDENT IDENTIFICATION

- ePHI Security Incident Severity Classification Table (Cont.)

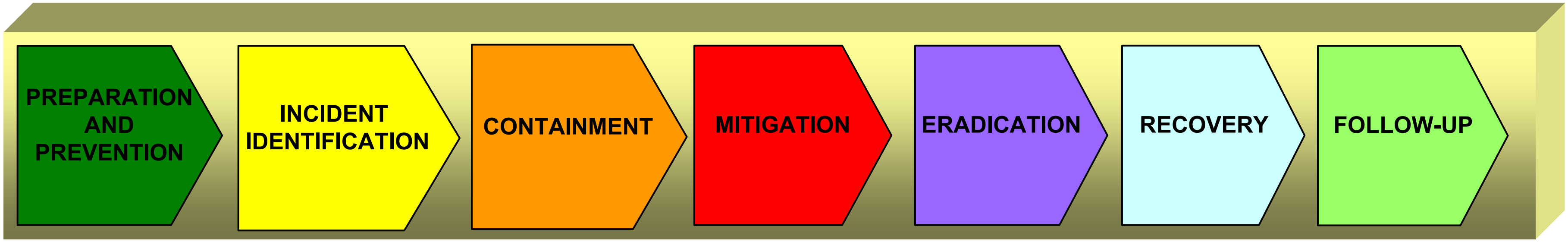
SEVERITY LEVEL	DESCRIPTION	EXAMPLE
2	Penetration or denial of service attacks attempted with limited impact on operations	Denial of service attacks executed against a workstation or web server
	Widespread instances of a new computer virus not handled by anti-virus software	Widespread trouble calls to the help desk reporting problems with Microsoft Outlook eventually found to be caused by the ILOVEYOU virus during its initial days
	Some risk to patient care or negative public relations impact	A CHCS terminal improperly located facing a high-traffic area. Concerns are brought to the staff attention by a patient
1	Successful penetration or denial of service attacks detected with significant impact on operations	Successful login to a router by an unauthorized personnel (internal or external) detected by the Network Administrator
	Significant risk to patient care or negative public relations impact	A workstation previously used by a provider is donated to a local school without properly erasing ePHI

HIPAA Security Incident Response Procedures

Incident Containment



- Containment involves short-term actions that are immediately implemented in order to limit the scope and magnitude of an HIPAA security incident

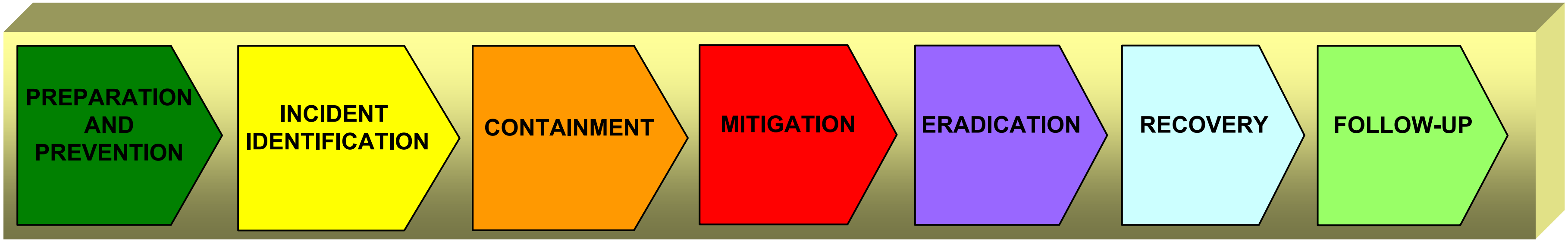


HIPAA Security Incident Response Procedures

Mitigation of Harmful Effects (1 of 5)

MITIGATION

- Develop a methodology for communicating with victims, investigators, senior leadership (both within the MHS and external), Congress, the media (both paper and television), law enforcement agencies, and other governmental parties
  - The methodology may range from sending letters to victims to using the Web site as the primary tool for providing up-to-date information



HIPAA Security Incident Response Procedures

Mitigation of Harmful Effects (2 of 5)

- OSD Memorandum 12282-05, to be incorporated in a future revision of DoDD 5400.11, states:
  - DoD Component shall inform the affected individuals as soon as possible, but no later than ten days after the loss or compromise of protected personal information is discovered
  - At a minimum, the DoD Component shall advise individuals of:
    - What specific data was involved
    - The circumstances surrounding the loss, theft, or compromise
    - What protective actions the individual can take

HIPAA Security Incident Response Procedures

Mitigation of Harmful Effects (3 of 5)

MITIGATION

- Mitigation activities include, at a minimum, the following:
  - Notifying all affected individuals
    - For victims that have had ePHI disclosed or if a victim is a senior level person, one should consider notification as expeditiously as possible (phone)
    - Initial contact with the victim should provide them with a brief synopsis of the impact of the incident, and what steps they should take to mitigate personal risk

HIPAA Security Incident Response Procedures

Mitigation of Harmful Effects (4 of 5)

- Mitigation activities include, at a minimum, the following (Cont.):
  - Establish a toll-free number for call-in purposes
  - Establish a Web site (Intranet-based) for beneficiary communication
  - Establish a centrally managed e-mail address for victims
  - Assign a representative to speak to the public

HIPAA Security Incident Response Procedures

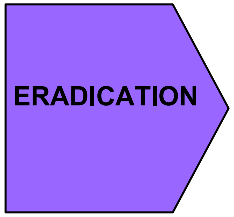
Mitigation of Harmful Effects (5 of 5)

- Stakeholder and Notification Methodology Table

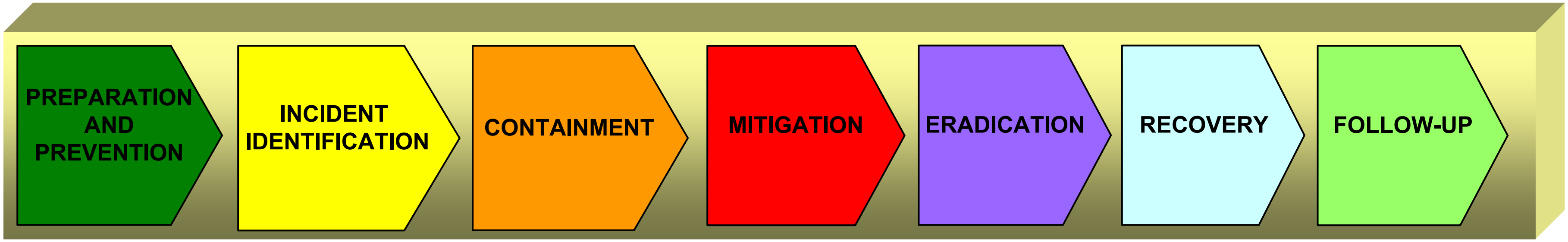
STAKEHOLDER ENTITY	METHODOLOGY
Victims whose individually identifiable health information has been accessed inappropriately	a. Information letter via U.S. mail b. Incident-specific Web site c. 1-800 number for questions and answers
Senior Leadership – examples include: DoD Senior Leadership (as determined by Service/MHS Senior Leaders) Army, Navy, Air Force Medical Departments	a. Phone (initial contact) b. E-mail message
General Counsel/Judge Advocate General	a. Initial contact by phone, followed by b. E-mail
Computer Incident Response Team (CIRT)	a. Initial contact by phone, followed by b. E-mail c. Meetings

HIPAA Security Incident Response Procedures

Eradication



- Eradication entails removing the cause of a security incident and mitigating vulnerabilities pertaining to the incident

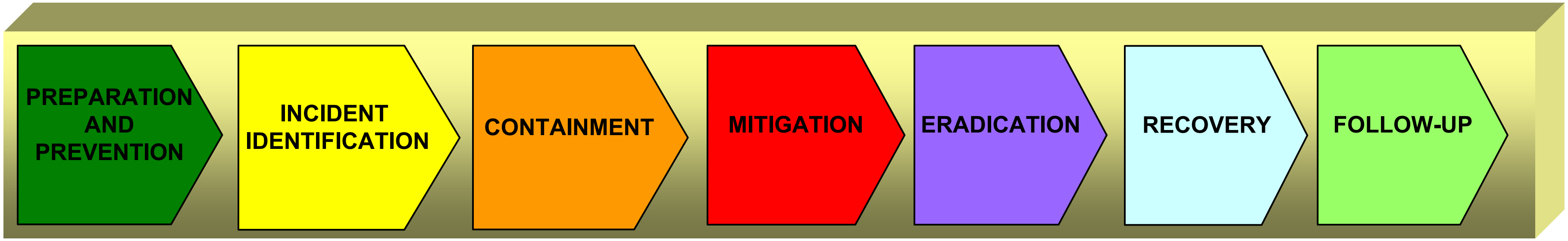


HIPAA Security Incident Response Procedures

Recovery

RECOVERY

- Recovery is the process of restoring to normal the status that existed prior to the occurrence of the security incident

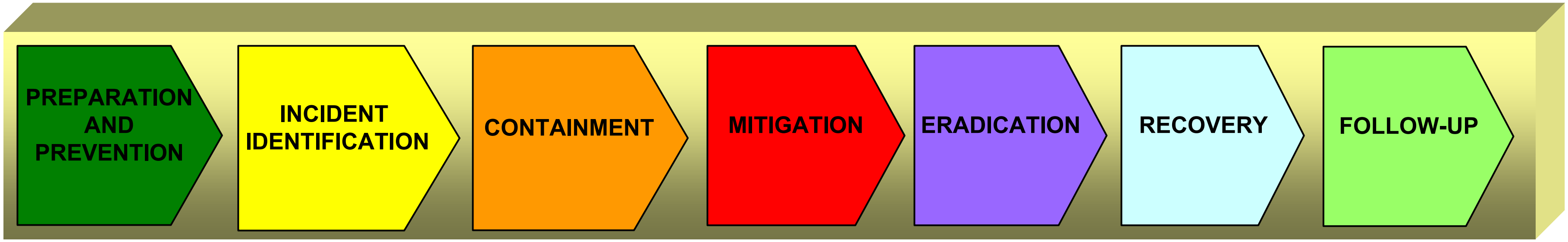


FOLLOW-UP

HIPAA Security Incident Response Procedures

Follow-Up

- Follow-up is a critical step in the security incident response process because it assists with the response to, and prevention of, future incidents



PREPARATION AND PREVENTION

INCIDENT IDENTIFICATION

CONTAINMENT

MITIGATION

ERADICATION

RECOVERY

FOLLOW-UP

HIPAA Security Incident Response Procedures

Summary

- You should now be able to:
  - Identify the types of security incidents that qualify as reportable incidents and, based upon the severity of the event, require notification of officials within TMA/MHS

HIPAA Security Incident Reporting

HIPAA Security Incident Reporting

Objectives

- Upon completion of this module you should be able to:
  - Outline the structure and process for reporting HIPAA security incidents

HIPAA Security Incident Reporting

Reporting (1 of 10)

- Incident reporting pertains to timely dissemination of information when a security incident occurs

- The organizational security incident response plan should include a communication strategy and methodology for notifying and updating concerned individuals at all levels of the organization when a security incident occurs

HIPAA Security Incident Reporting

Reporting (2 of 10)

- Reporting activities include, at a minimum, the following:
  - Develop a process and procedures for reporting security incidents and communicating situational updates, as necessary
  - Identify a point of contact at each level of the organization to serve as the lead in reporting security incidents to the appropriate officials

HIPAA Security Incident Reporting

Reporting (3 of 10)

- Reporting activities include, at a minimum, the following (Cont.):
  - Report HIPAA security incidents classified as severity level 1 or 2 via the local, regional, and Service Medical Headquarters chain of command to the MHS HA/TMA IA Program Office using the format provided in the MHS HIPAA Security Incident Response Plan

HIPAA Security Incident Reporting

Reporting (4 of 10)

- Reporting activities include, at a minimum, the following (Cont.):
  - Forward a report of security incidents classified as level 3, 4 or 5 to the MHS HA/TMA IA Program Office on a quarterly basis
  - Follow existing local and higher authority guidance regarding additional security incident reporting requirements

HIPAA Security Incident Reporting

Reporting (5 of 10)

- Reporting Matrix

REPORTING ENTITY	SEVERITY LEVEL 5-3	SEVERITY LEVEL 2	SEVERITY LEVEL 1
MTF	Quarterly to SG through chain of command. No verbal.	Verbal to SG in 24 hours with verbal updates every 24 hours until under control. Weekly written updates until resolved.	Verbal to SG in 24 hours with verbal updates every 24 hours until under control. Weekly written updates until resolved.
SG	Quarterly to MHS HA/TMA IA PO. No verbal.	Monthly to MHS HA/TMA IA PO when it involves centrally managed systems or crosses services. Rest aggregate quarterly. No verbal.	Immediate notification to MHS HA/TMA IA PO with timely verbal and written updates.
MHS HA/TMA IA PO	MHS HA/TMA IA PO does NOT forward to TMA PO.	Monthly to TMA PO when it involves centrally managed systems or crosses services.	Immediate notification to TMA PO with timely verbal and written updates.

HIPAA Security Incident Reporting

Reporting (6 of 10)

- Reporting ePHI Security Incidents Table

SEVERITY LEVEL	IMMEDIATE MHS HA/TMA IA PROGRAM OFFICE REQUIRED			ACTIONS
	VERBAL	WRITTEN	UPDATE	
5	No.	No. Report of Level 5 activity is required on a quarterly basis to TMA	No.	1. Compile a report of Level 5 incidents using the format provided by TMA. 2. Forward quarterly aggregate report of Level 5 security incidents via local, regional, and service level Point of Contacts (POCs), as appropriate, to the MHS HA/TMA IA Program Office at: (E-mail address) (Fax number) 3. Maintain documentation of the incident.

HIPAA Security Incident Reporting

Reporting (7 of 10)

- Reporting ePHI Security Incidents Table (Cont.)

SEVERITY LEVEL	IMMEDIATE MHS HA/TMA IA PROGRAM OFFICE REQUIRED			ACTIONS
	VERBAL	WRITTEN	UPDATE	
4	No.	No. Report of Level 4 activity is required on a quarterly basis to TMA	No.	1. Compile a report of Level 4 incidents using the format provided by TMA. 2. Forward quarterly aggregate report of Level 4 security incidents via local, regional, and service level Point of Contacts (POCs), as appropriate, to the MHS HA/TMA IA Program Office at: (E-mail address) (Fax number) 3. Maintain documentation of the incident.

HIPAA Security Incident Reporting

Reporting (8 of 10)

- Reporting ePHI Security Incidents Table (Cont.)

SEVERITY LEVEL	IMMEDIATE MHS HA/TMA IA PROGRAM OFFICE REQUIRED			ACTIONS
	VERBAL	WRITTEN	UPDATE	
3	No.	No. Report of Level 3 activity is required on a quarterly basis to TMA	No.	1. Compile a report of Level 3 incidents using the format provided by TMA. 2. Forward quarterly aggregate report of Level 3 security incidents via local, regional, and service level Point of Contacts (POCs), as appropriate, to the MHS HA/TMA IA Program Office at: (E-mail address) (Fax number) 3. Maintain documentation of the incident.

Reporting (9 of 10)

- Reporting ePHI Security Incidents Table (Cont.)

SEVERITY LEVEL	IMMEDIATE MHS HA/TMA IA PROGRAM OFFICE REQUIRED			ACTIONS
	VERBAL	WRITTEN	UPDATE	
2	No. However, notify Service Medical Headquarters through the appropriate chain of command within 24 hours of incident.	No. However, Service Medical Headquarters will report to the MHS HA/TMA Program Office on a monthly basis if incident involves the centrally managed systems or systems and/or ePHI owned by other Services. The Service Medical Headquarters will report to the MHS HA/TMA Program Office all other level 2 incidents on a quarterly basis.	No. However, notify Service Medical Headquarters every 24 hours verbally until the incident is under control, and provide a weekly written update until incident is resolved.	1. Ensure that appropriate chain of command at the local, regional and service headquarters level is notified of Level 2 security incidents. 2. The Service HIPAA Compliance Representative within each Service Medical Department will notify the MHS HA/TMA IA Program Office on a monthly basis if incident involves the centrally managed systems or systems and/or ePHI owned by other Services. at: (E-mail address) (Fax number) (Telephone Number) 3. Maintain documentation of the incident.

HIPAA Security Incident Reporting

Reporting (10 of 10)

- Reporting ePHI Security Incidents Table (Cont.)

SEVERITY LEVEL	IMMEDIATE MHS HA/TMA IA PROGRAM OFFICE REQUIRED			ACTIONS
	VERBAL	WRITTEN	UPDATE	
1	Yes, within 24 hours of incident.	Yes, within 24 hours of verbal communication.	Yes, every 24 hours verbally until incident is under control, and weekly written update until incident is resolved.	1. Ensure that appropriate chain of command at the local, regional and service headquarters level is notified of Level 1 security incidents using the format provided by TMA. 2. The Service HIPAA Compliance Representative within each Service Medical Department will immediately notify the MHS HA/TMA IA Program Office at: (E-mail address) (Fax number) (Telephone Number) 3. Maintain documentation of the incident.

Incident Response Plan

Summary

- You should now be able to:
  - Identify some of the key responsibilities and duties of the organizational staff that may be involved in managing and reporting HIPAA security incidents
  - Identify the types of security incidents that qualify as reportable incidents and, based upon the severity of the event, require notification of officials within TMA
  - Outline the structure and process for reporting HIPAA security incidents

Measuring Effectiveness

Training Objectives

- Upon completion of this course you should be able to:
  - Understand the elements of oversight for HIPAA security implementation
  - Identify processes and areas of your organization that contribute to measuring the effectiveness of ongoing HIPAA security compliance
  - Recognize possible areas of improvement of compliance and management of HIPAA security
  - Identify some of the key aspects involved in measuring ongoing compliance and management of HIPAA security

Background Information

Requirement

- An administrative safeguard specified in the HIPAA Security Regulation requires
  - An annual (at a minimum) technical and non-technical evaluation of the security **program** and in response to environmental or operational changes affecting the security of electronic PHI
  - Establishing the **extent** to which the organization's security policies and procedures meet the requirements of this regulation

Background Information

Mandate

- Authority
  - DoD 6025.18-D, Privacy of Individually Identifiable Health Information in DoD Health Care Programs
    - The responsibilities of MHS covered entities shall be construed as **responsibilities** of the MHS, under the management control of the Director, TRICARE Management Activity
  - DoD 8580.X-D (Draft), Security of Individually Identifiable Health Information in DoD Health Care Programs
    - The Assistant Secretary of Defense (Health Affairs), under the Under Secretary of Defense (Personnel and Readiness), shall exercise **oversight** to ensure compliance

Background Information

Oversight Responsibilities

- Management control and oversight of the MHS covered entities includes:
  - Provide guidance on implementation
  - Assess the effectiveness
  - Facilitate mitigation and improvement

Background Information

Oversight Requirements

- To ensure oversight and compliance you need information on:
  - Immediate status of critical requirements
  - Operational data to facilitate accountability and issue resolution
  - Measures of program effectiveness

HIPAA Security Reporting Elements

HIPAA Security Reporting Elements

Objectives

- Upon completion of this module you should be able to:
  - Identify key elements involved in compliance issue awareness and resolution
  - Identify the source, content, and requirements for reporting of key elements that require notification of officials within TMA/MHS

Reporting Element Requirements

- Compliance issue awareness and resolution are required for accountability and timely mitigation

- In order to obtain the status of critical requirements and operational data to facilitate accountability and issue resolution, you need:
  - Regular compliance status reports
  - Who is accountable for issue resolution in the field
  - Process for reporting and tracking incidents and complaints

HIPAA Security Reporting Elements

Types of Reporting Elements

- Security Officer Report
- Training Report
- HIPAA BASICS$^{\text{TM}}$
- OCTAVE$^{\text{SM}}$ Report
- Incident Reports
- Complaint Reports

HIPAA Security Reporting Elements

Security Officer Report

- Source: Manual reports from each MTF

- Content:
  - Baseline report for each facility
    - Name and contact information
    - Current tenure
    - Training details
  - Turnover report
    - New name and contact information
    - Tenure of exiting officer
    - Training plan

HIPAA Security Reporting Elements

Training Report

- Source: Learning Management System (LMS)
- Content:
    - Percentage of workforce trained
    - Percentages based on 30, 60, and 90 day delinquency rates

HIPAA Security Reporting Elements

HIPAA BASICS^{TM}

- Source: HIPAA BASICS^{TM}

- Content:
  - Average compliance rate
  - Detailed requirement status
  - # of gaps updated in current calendar year
  - # of gaps currently being updated
  - # of risk assessments older than 1 year
  - # of risk assessments updated in current calendar year
  - # of risk assessments currently being updated

HIPAA Security Reporting Elements
OCTAVE^{SM} Report

- Source: OCTAVE^{SM} Report / RIMR database
  - Future reporting

- Content:
  - Percentage of MTFs using OCTAVE^{SM}
  - Other content TBD
  - # of risk assessments older than 1 year
  - # of risk assessments updated in current calendar year
  - # of risk assessments currently being updated

HIPAA Security Reporting Elements

Incident Reports

- Source: Manual reports from each MTF
- Content:
  - Report content and format defined in the MHS HIPAA Security Incident Response Plan
    - Quarterly reports of HIPAA security incidents classified as level 1, 2, and 3
    - Immediate reports of HIPAA security incidents classified as level 4 and 5

HIPAA Security Reporting Elements

Complaint Reports

- Source: Manual reports from each MTF
- Content
  - Number of complaints received in last reporting interval
  - Number of complaints held over from previous reporting intervals
  - Initial and updated complaints include the following detail:
    - Complaint type
    - Source of complaint
    - # validated security complaints
    - # complaints still being validated
    - # determined to not be valid security complaints

HIPAA Security Reporting Elements

Reporting Requirements

- The details of the reports for each reporting element include
  - Format
  - Frequency
  - Chain of Reporting
  - Starting date
- Reporting requirements will be disseminated through Service Representatives

HIPAA Security Reporting Elements

Summary

- You should now be able to:
  - Identify key elements involved in compliance issue awareness and resolution
  - Identify the source, content, and requirements for reporting of key elements that require notification of officials within TMA/MHS

HIPAA Security Metrics

HIPAA Security Metrics

Objectives

- Upon completion of this module you should be able to:
  - Recognize characteristics of metrics for measuring the management of and compliance with HIPAA security
  - Identify the components of a HIPAA security effectiveness report, which supplements existing compliance reports
  - Assess, analyze, and validate compliance with HIPAA security implementation by regions or across the entire Service

HIPAA Security Metrics

Requirement

- Security and Privacy goals are met by the integration of people, processes, procedures, and tools

- In order to measure program effectiveness, you need to:
  - Gauge ongoing management of people, processes, procedures, and tools supporting HIPAA requirements
  - Extend existing self-assessment reports of compliance
  - Establish basis for review of compliance by external teams

HIPAA Security Metrics

Approach

- Each Standard and Implementation Specification was reviewed for administrative, physical, and technical processes that support HIPAA security compliance throughout an organization
- A metric was created for each that draws on qualitative and quantitative aspects of HIPAA security implementation
- Each metric serves to assist in (1) gauging effectiveness, and (2) guiding in the improvement of information assurance activities related to HIPAA security

HIPAA Security Metrics

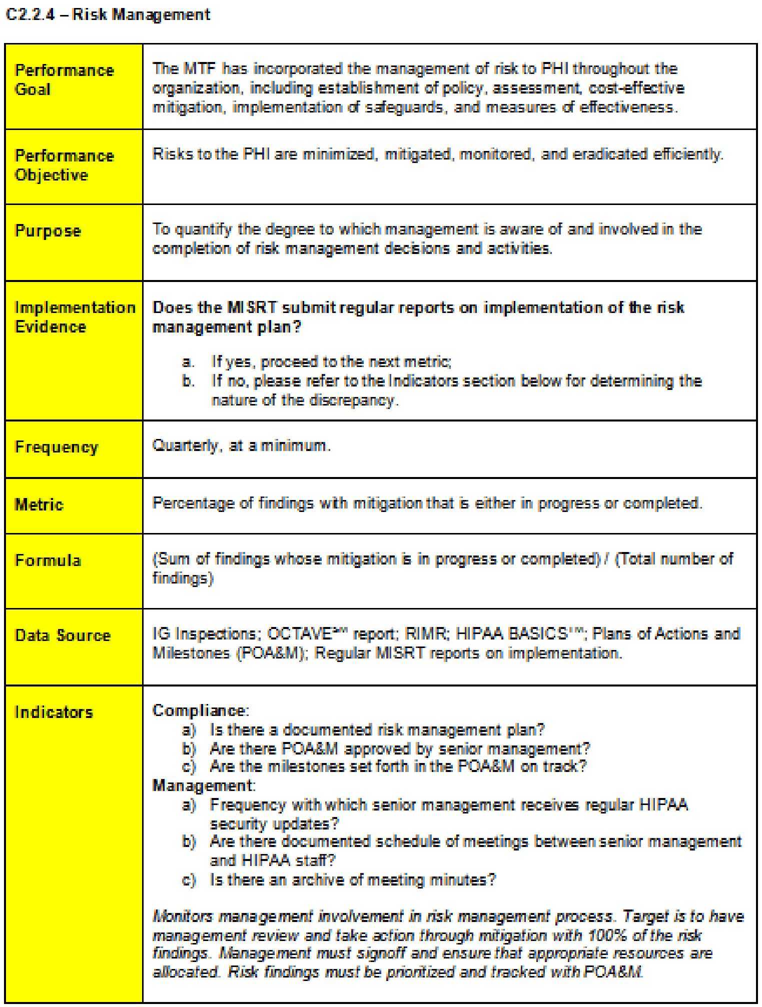
Purpose

- The following metrics and methodology
  - Provide a basis for ongoing measure of management and compliance by integrating qualitative and quantitative measures across technical, administrative, and physical areas
  - Produce a report to supplement the existing compliance reports and the Compliance Assurance Framework
  - Assist organizations improve their IA security posture

HIPAA Security Metrics

Details and Illustration

- A description of the components of each metric follows:
  - Performance Goal
  - Performance Objective
  - Purpose
  - Implementation Evidence
  - Frequency
  - Metric
  - Formula
  - Data Source
  - Indicators of Compliance
  - Indicators of Management



C2.2.4 – Risk Management

Performance Goal	The MTF has incorporated the management of risk to PHI throughout the organization, including establishment of policy, assessment, cost-effective mitigation, implementation of safeguards, and measures of effectiveness.
Performance Objective	Risks to the PHI are minimized, mitigated, monitored, and eradicated efficiently.
Purpose	To quantify the degree to which management is aware of and involved in the completion of risk management decisions and activities.
Implementation Evidence	**Does the MISRT submit regular reports on implementation of the risk management plan?** a. If yes, proceed to the next metric; b. If no, please refer to the Indicators section below for determining the nature of the discrepancy.
Frequency	Quarterly, at a minimum.
Metric	Percentage of findings with mitigation that is either in progress or completed.
Formula	(Sum of findings whose mitigation is in progress or completed) / (Total number of findings)
Data Source	IG Inspections; OCTAVE℠ report; RIMR; HIPAA BASICS™; Plans of Actions and Milestones (POA&M); Regular MISRT reports on implementation.
Indicators	**Compliance:** a) Is there a documented risk management plan? b) Are there POA&M approved by senior management? c) Are the milestones set forth in the POA&M on track? **Management:** a) Frequency with which senior management receives regular HIPAA security updates? b) Are there documented schedule of meetings between senior management and HIPAA staff? c) Is there an archive of meeting minutes? *Monitors management involvement in risk management process. Target is to have management review and take action through mitigation with 100% of the risk findings. Management must signoff and ensure that appropriate resources are allocated. Risk findings must be prioritized and tracked with POA&M.*

HIPAA Security Metrics

Performance Goal

Performance Goal	Example: Risk Management
The desired results of implementing one or several HIPAA security objectives / techniques that are measured by the metric.	The MTF has incorporated the management of risk to PHI throughout the organization, including establishment of policy, assessment, cost-effective mitigation, implementation of safeguards, and measures of effectiveness.

HIPAA Security Metrics

Performance Objective

Performance Objective	Example: Risk Management
The actions that are required to accomplish the performance goal. Multiple performance objectives can correspond to a single performance goal.	Risks to the PHI are minimized, mitigated, monitored, and eradicated efficiently.

Purpose

Purpose	Example: Risk Management
Overall functionality obtained by collecting the metric. Includes whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.	To quantify the degree to which management is aware and involved in the completion of risk management decisions and activities.

Implementation Evidence

Implementation Evidence	Example: Risk Management
List proof of the security controls' existence that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric.	Does the MISRT submit regular reports on implementation of the risk management plan?

HIPAA Security Metrics

Frequency

Frequency	Example: Risk Management
Proposed time periods for collection of data that is used for measuring changes over time. Time periods based on likely updates occurring in the control implementation.	Quarterly, at a minimum.

HIPAA Security Metrics

Metric

Metric	Example: Risk Management
The quantitative measurement provided by the metric.	Percentage of findings with mitigation either in progress or completed.

HIPAA Security Metrics

Formula

Formula	Example: Risk Management
The calculation to be performed that results in a numeric expression of a metric. The information gathered through listing implementation evidence serves as an input into the formula for calculating the metric.	(Sum of findings whose mitigation is in progress or completed) / (Total number of findings).

HIPAA Security Metrics

Data Source

Data Source	Example: Risk Management
List the location of the data to be used in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.	IG Inspections; OCTAVE^{SM} report; RIMR; self-assessment report; Plans of Actions and Milestones (POA&M), Regular MISRT reports on implementation.

HIPAA Security Metrics

Indicators of Compliance

Indicators of Compliance	Example: Risk Management
Minimal, qualitative safeguards for meeting HIPAA security requirements. Reflects what must be in place.	a) Is there a documented risk management plan? b) Is the POA&M approved by senior management? c) Are the milestones set forth in the POA&M on track?

HIPAA Security Metrics

Indicators of Management

Indicators of Management	Example: Risk Management
Characteristics and type of processes that support the management of HIPAA security safeguards. Highlights cultural aspects of successful HIPAA security implementation.	a) Frequency senior management receives regular HIPAA security updates? b) Is there a documented schedule of meetings between senior management and HIPAA staff? c) Is there an archive of meeting minutes?

Measuring Ongoing Effectiveness

MTF Use of Metrics

- An inspection report based on the HIPAA security metrics and associated methodology presented provides the basis for an assessment and validation of compliance with HIPAA security implementation
- The results of the inspection reports are provided to the MTF senior management for review and corrective action
- Metrics are required annually

Measuring Ongoing Effectiveness

Service Use of Metrics

- Individual reports can be used to assess MTF compliance and management of HIPAA security

- Aggregate reports can track compliance by regions or across the entire Service

- All reports allow trend analysis at MTFs, regions, and across the Services

Measuring Ongoing Effectiveness

TMA Use of Metrics

- TMA receives aggregate Service reports to gauge effectiveness of HIPAA implementation across each Service and the MHS

- Aggregate reports are created by
  - Designating compliance with each metric by “Yes” or “No”
  - Aggregating each metric across each Service
  - Calculating percentages based on aggregate results
  - Reporting results on effectiveness, which complement the existing self-assessment reports

Measuring Ongoing Effectiveness

Aggregate Report Illustration

Metric	MTF 1	MTF 2	MTF 3	MTF 4	Aggregate
Risk Management	1	0	1	1	¾ = 75%
Incident Response	0	0	1	0	¼ = 25%

Measuring Effectiveness

Summary

- You should now be able to:
  - Understand the elements of oversight for HIPAA security implementation
  - Identify processes and areas of your organization that contribute to measuring the effectiveness of ongoing HIPAA security compliance
  - Recognize possible areas of improvement of compliance and management of HIPAA security
  - Identify some of the key aspects involved in measuring ongoing compliance and management of HIPAA security

Training Summary

- You should now be able to:
  - Identify the individuals and steps involved during a HIPAA security incident under the MHS HIPAA Security Incident Response Plan
  - Classify and report HIPAA security incidents as described in the MHS HIPAA Security Incident Response Plan
  - Measure and improve compliance with and management of HIPAA security

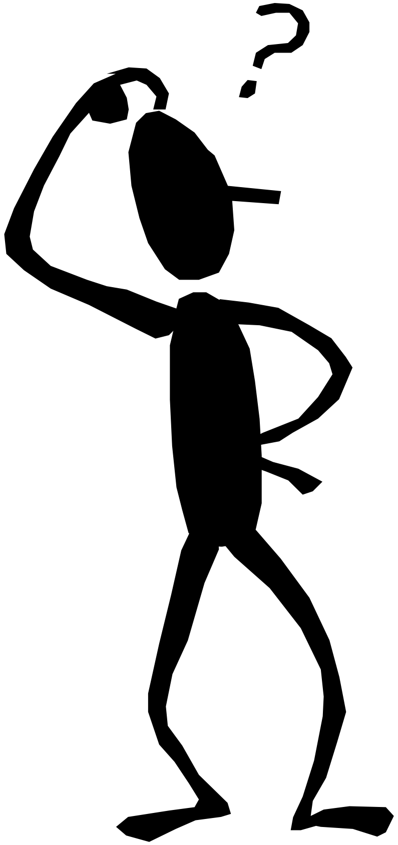
Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- MHS HIPAA Security Incident Response Plan, May 2005
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm to subscribe to the TMA Privacy Office E-News
- HIPAA Security Service Representatives

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- MHS HIPAA Security Incident Response Plan, May 2005
- www.tricare.osd.mil/hipaa/privacy
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm to subscribe to the TMA Privacy Office E-News
- Service HIPAA security representatives

Questions



Please fill out your critique

Thanks!